Russian attacks on civilian infrastructure in Ukraine: UK statement to the OSCE

Thank you, Madam Chair, again for convening us today and bringing together panel experts for such a timely discussion that has highlighted the impacts on civilians when critical services are damaged, as well as the role of States in protecting these services in armed conflict.

As has been noted several times today but cannot be overstated, a little over a year ago, Russia joined with others at the UN Security Council to unanimously adopt Resolution 2573. Yet, in a flagrant breach of International Humanitarian Law, Russian bombers have, in recent weeks, repeatedly and remorselessly dropped targeted munitions on civilian infrastructure in Ukraine, including government buildings, hospitals, schools, and transportation.

Today we have heard the numbers of verified attacks on Ukraine's health facilities. Stretched healthcare facilities in the East are having to respond to growing reports of gender-based violence, including Conflict-Related Sexual Violence. Earlier today, Prime Minister Johnson addressed Ukraine's Parliament, setting out a new package of military aid to enable Ukraine to defend itself as well as specialised civilian protection vehicles, and we will continue to provide humanitarian aid including generators to support vital services to keep running.

The dangers of this war transcend borders. As described by our keynote speaker, the world has witnessed concerning attacks on Ukrainian nuclear facilities, demonstrating Russia's reckless attitude to nuclear safety and security. The UK will continue to support neighbouring countries, including those which are hosting refugees. We continue to provide regional support in the cyber space, including by sharing threat information. For instance, we have recently launched our new programme supporting Georgia to implement its new National Security Strategy, focusing on incident management, information sharing, and the cyber awareness of vulnerable groups.

At times of heightened international tension all critical service providers must be vigilant to the risk of cyber compromises. Earlier this month, the UK joined our international partners to share updated mitigation advice against state-sponsored and criminal cyber threats. Strengthening the relationships between government departments, regulators, and private sector operators is key to ensuring the latest threats, risks and vulnerabilities are understood and mitigated effectively.

States should, where possible, make publicly available their approaches to cyber security and resilience, including how they relate to critical infrastructure protection. The UK routinely publishes this information including guides on how to effectively detect, respond to and resolve cyber

incidents, and crucially where organisations can find support from certified Cyber Incident Response companies assessed against clear published standards. Sharing best practice in approaches to critical infrastructure dependences and cooperating across borders are crucial elements of strengthening our international resilience.

Madam chair, we have entered a new world where service protection and resilience measures must not only be prepared to stand up to threats caused by non-state terrorist acts, but direct and targeted missile attack. As we enter the third month of President Putin’s illegal and unprovoked war, not only do thousands of civilians remain in Mariupol, Kherson, Donetsk, Luhansk, and other cities, struggling to survive without food, water, warmth, and medical supplies, but the effects continue to mount around the world. The OSCE has a role to play to prevent knock-on crises in crime, trafficking, and terrorism, and the UK stands ready to support the Security Committee to that end.

Thank you.